All sides of Android: il buono, il brutto, il cattivo

Tim Vidas

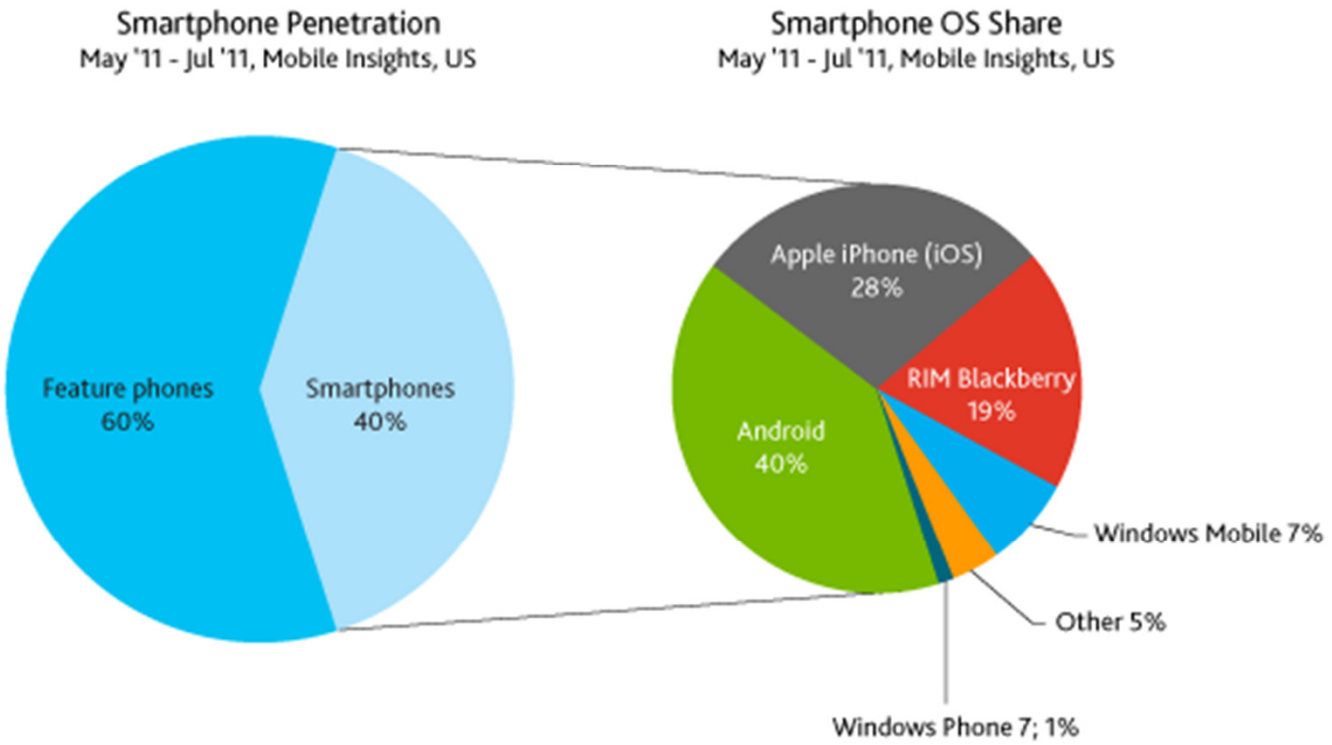
Dell SecureWorks

Agenda

Images from: United Artists; Google, Inc.

Why android?

Smartphones now make up 40% of all mobile phones in the US



Source: Nielsen

nielsen

Nielsen, Sept 2011

DELL SecureWorks

Why Android?

Android is a big player in the mobile smartphone arena.

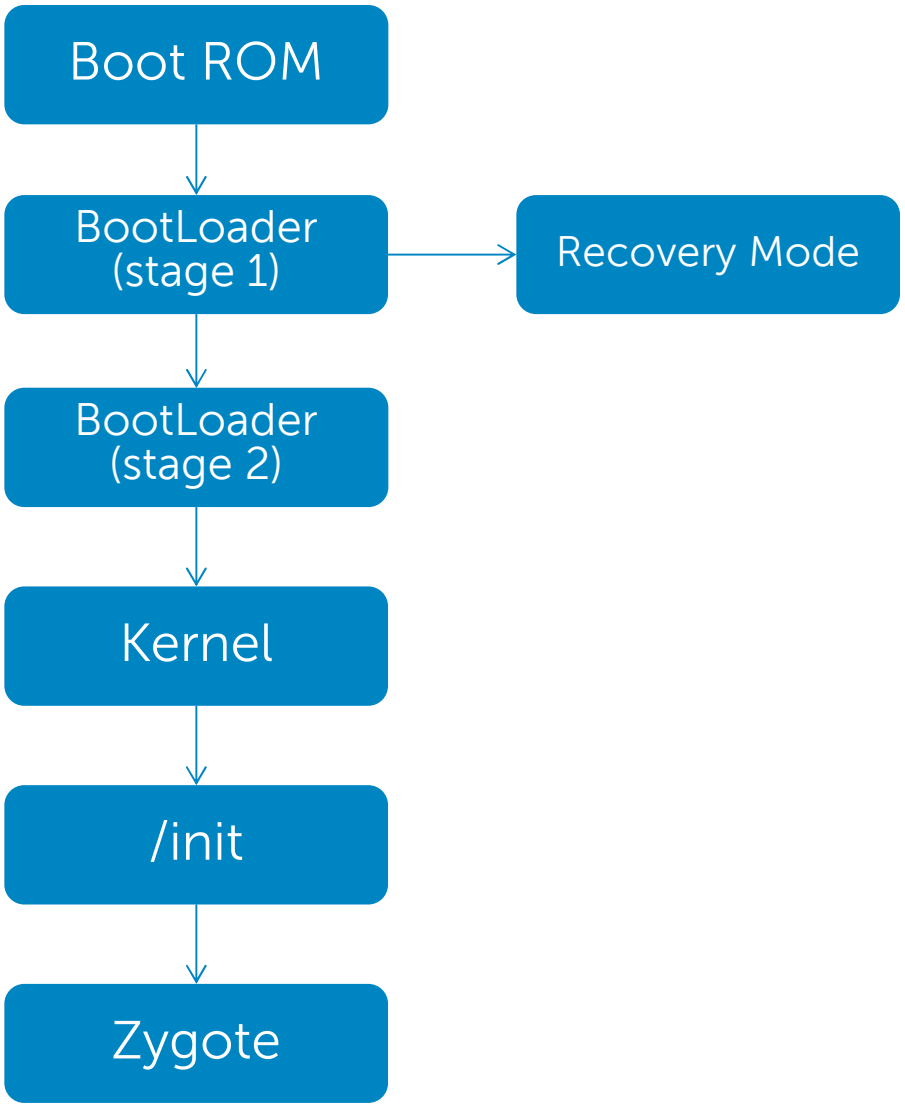
Every major carrier has multiple Android based devices

Android smartphones typically get some of the “latest and greatest” technologies, such as the newer 4G networks, NFC, and screens that are easier to see in daylight.

How it is: Basics

- Modern phones are as powerful as laptops
- Android around since ~2009
  - Different model than Apple, Blackberry, etc
  - Open market model (Apple “vets” apps)
  - Open source project (mostly)
  - Applications have special “app level permissions”’
- None allow you to really administer your device

How it is: Boot Process

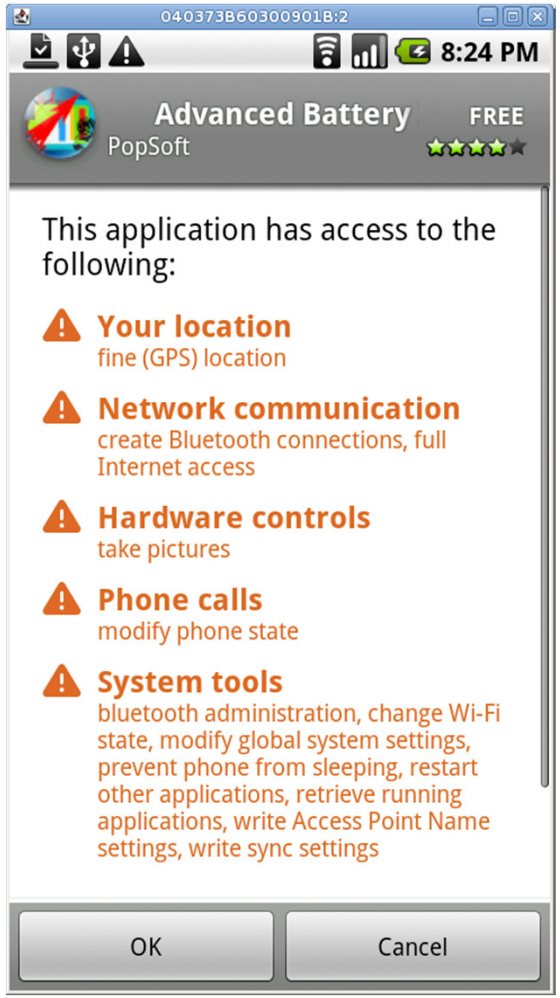


- Much like a typical Linux boot process
- Apps are run in a JVM, but the seperation is provided by Linux
- Boot process is unauthenticated and can be hijacked

How it is: Partition Layout

Path	Name	FS	Mount Pt	Description
/dev/mtd/mtd0	Pds	yaffs2	/config	Config data
/dev/mtd/mtd1	misc			Memory partitioning data
/dev/mtd/mtd2	boot	bootimg		Typical boot image
/dev/mtd/mtd3	recovery	bootimg		Recovery mode boot image
/dev/mtd/mtd4	system	yaffs2	/system	System files, system apps, etc
/dev/mtd/mtd5	cache	yaffs2	/cache	Cache files
/dev/mtd/mtd6	userdata	yaffs2	/data	User data (apps, settings, etc)
/dev/mtd/mtd7	kpanic			Crash Log

How it is: App permissions



- Access to system resources are granted through application level permissions
- People tend to disregard them

BRICK
BROADCAST_PACKAGE_REMOVED
BROADCAST_SMS
BROADCAST_STICKY
BROADCAST_WAP_PUSH
CALL_PHONE
CALL_PRIVILEGED
CAMERA
CHANGE_COMPONENT_ENABLED_STATE
CHANGE_CONFIGURATION
CHANGE_NETWORK_STATE
CHANGE_WIFI_MULTICAST_STATE
CHANGE_WIFI_STATE
CLEAR_APP_CACHE
CLEAR_APP_USER_DATA
CONTROL_LOCATION_UPDATES
DELETE_CACHE_FILES
DELETE_PACKAGES
DEVICE_POWER
DIAGNOSTIC
DISABLE_KEYGUARD
DUMP
EXPAND_STATUS_BAR
FACTORY_TEST
FLASHLIGHT
FORCE_BACK
GET_ACCOUNTS
GET_PACKAGE_SIZE
GET_TASKS

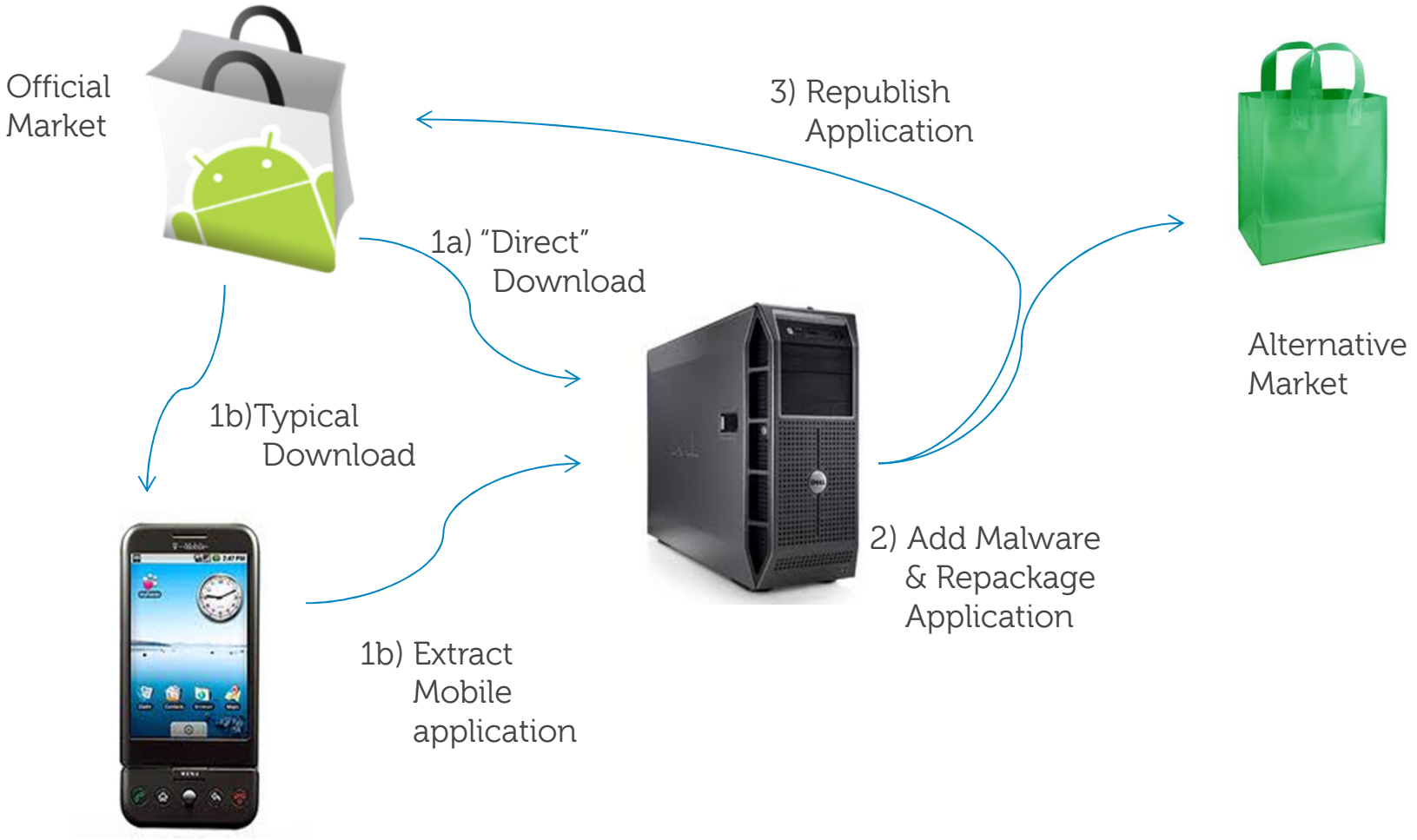
How it is: App permissions

- Bad combos
  - SMS when not needed
  - READ_LOGS supersedes many permissions
  - INTERNET and READ_CONTACTS
  - INTERNET and INSTALL_PACKAGES
  - INTERNET and ALMOST_EVERYTHING
  - Unfortunately many free apps require network so ads can be retrieved

Bad apps

- Spoofed
  - Netflix
- Repackaged / grafted
  - MonkeyJump
- Spyware
  - Stealth *
- Greyware
  - Almost everything else
- Rooting
  - Is ok, but some apps do it when you don't know
  - RootSmart

Repackaging



Unlike typical malware…

- Most malware is delivered from a portal known as a market place
  - By default phones don't allow sources other than the official
  - Apps can be set to start automatically after boot, upon SMS arrival, upon installation of another app, really a lot of different events (intents)
- Your phone might come with bad stuff on it
  - As HTC nicely demonstrated with an unauthenticated port

What are the percents really?

- Official market
  - REALLY low
  - Like a small fraction of a percent

- Alternative markets
  - All over the place

Quick Malware Tour: Zitmo

Trusteer Building trust online

Dear Customer!

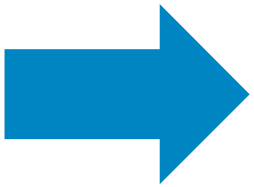
Trusteer is glad to announce the new mobile app which protects your phone while working with online banking, receiving and sending SMS and making calls.

Over 22 millions customers, banks and financial instututions use our programm software to make payments, transfers and other operations securely. If you're working with our software, your security is protected by professionals.

Please chose your phone's operating system:

- ○ iOS (iPhone)
- ○ BlackBerry
- ◉ Android
- ○ Symbian (Nokia)
- ○ Other

Continue



Please download "tr.apk"

Quick Malware Tour: Spoof

- Netflix only supports certain devices.
- But "Netflix" is available for every device!!

Image: Symantec

Quick Malware Tour: Repackaged

- Geinimi
- MonkeyJump

android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.VIBRATE

Quick Malware Tour: Repackaged

- Geinimi
- MonkeyJump

android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.VIBRATE
com.android.launcher.permission.INSTALL_SHORTCUT
android.permission.ACCESS_FINE_LOCATION
android.permission.CALL_PHONE
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.READ_CONTACTS
android.permission.READ_SMS
android.permission.SEND_SMS
android.permission.SET_WALLPAPER
android.permission.WRITE_CONTACTS
android.permission.WRITE_EXTERNAL_STORAGE
com.android.browser.permission.READ_HISTORY_BOOKM
com.android.browser.permission.WRITE_HISTORY_BOOKM
android.permission.ACCESS_GPS
android.permission.ACCESS_LOCATION
android.permission.RESTART_PACKAGES
android.permission.RECEIVE_SMS
android.permission.WRITE_SM

```
<intent-filter android:priority="65535">
        <action android:name="android.provider.Telephony.SMS_RECEIVED">
        </action>
</intent-filter>
```

Quick Malware Tour: Repackaged

- DroidDream

* Falling Down
* Super Guitar Solo
* Super History Eraser
* Photo Editor
* Super Ringtone Maker
* Super *** Positions
* Hot ***y Videos
* Chess
* 下坠 滚球_Falldown
* Hilton *** Sound
* Screaming ***y Japanese Girls
* Falling Ball Dodge
* Scientific Calculator
* Dice Roller
* 躲避 弹球
* Advanced Currency Converter
* App Uninstaller
* 几何 战机_PewPew
* Funny Paint
* Spider Man
* 蜘蛛 侠

Quick Malware Tour: Repackaged

- DroidDream

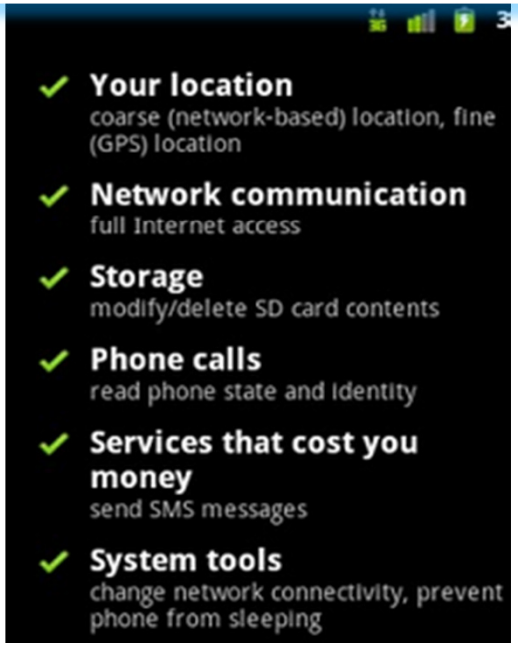
* Falling Down
* Super Guitar Solo
* Super History Eraser
* Photo Editor
* Super Ringtone Maker
* Super *** Positions
* Hot ***y Videos
* Chess
* 下坠 滚球_Falldown
* Hilton *** Sound
* Screaming ***y Japanese Girls
* Falling Ball Dodge
* Scientific Calculator
* Dice Roller
* 躲避 弹球
* Advanced Currency Converter
* App Uninstaller
* 几何 战机_PewPew
* Funny Paint
* Spider Man
* 蜘蛛 侠

Quick Malware Tour: Repackaged

- DroidDream

* Falling Down
* Super Guitar Solo
* Super History Eraser
* Photo Editor
* Super Ringtone Maker
* Super *** Positions
* Hot ***y Videos
* Chess
* 下坠 滚球_Falldown
* Hilton *** Sound
* Screaming ***y Japanese Girls
* Falling Ball Dodge
* Scientific Calculator
* Dice Roller
* 躲避 弹球
* Advanced Currency Converter
* App Uninstaller
* 几何 战机_PewPew
* Funny Paint
* Spider Man
* 蜘蛛 侠

Fake Android Market Security tool delivers more than just a cure for Droid Dream malware



Quick Malware Tour: Rooting

- RootSmart
  - Repackaged
  - Does not bundle root exploit (which might be caught by antivirus)

ACCESS_FINE_LOCATION
ACCESS_NETWORK_STATE
ACCESS_WIFI_STATE
BLUETOOTH
BLUETOOTH_ADMIN
CAMERA
CHANGE_WIFI_STATE
FLASHLIGHT
GET_ACCOUNTS
HARDWARE_TEST
MODIFY_PHONE_STATE
READ_SECURE_SETTINGS
READ_SYNC_SETTINGS
RECEIVE_BOOT_COMPLETED
VIBRATE
WAKE_LOCK
WRITE_APN_SETTINGS
WRITE_SECURE_SETTINGS
WRITE_SETTINGS
WRITE_SYNC_SETTINGS

Quick Malware Tour: Rooting

- RootSmart
  - Repackaged
  - Does not bundle root exploit (which might be caught by antivirus)
  - Instead dynamically downloads GingerBreak
    - Additional permissions
  - Reacts to several phone actions

ACCESS_CACHE_FILESYSTEM
ACCESS_FINE_LOCATION
ACCESS_NETWORK_STATE
ACCESS_WIFI_STATE
BLUETOOTH
BLUETOOTH_ADMIN
CAMERA
CHANGE_CONFIGURATION
CHANGE_WIFI_STATE
DELETE_CACHE_FILES
DEVICE_POWER
FLASHLIGHT
GET_ACCOUNTS
GET_TASKS
HARDWARE_TEST
INTERNET
MODIFY_PHONE_STATE
MOUNT_UNMOUNT_FILESYSTEMS
READ_LOGS
READ_OWNER_DATA
READ_PHONE_STATE
READ_SECURE_SETTINGS
READ_SYNC_SETTINGS
RECEIVE_BOOT_COMPLETED
RESTART_PACKAGES
SYSTEM_ALERT_WINDOW
VIBRATE
WAKE_LOCK
WRITE_APN_SETTINGS
WRITE_EXTERNAL_STORAGE
WRITE_OWNER_DATA
WRITE_SECURE_SETTINGS
WRITE_SECURE_SETTINGS
WRITE_SETTINGS
WRITE_SYNC_SETTINGS

Analysis: get an app

- Download to device then extract via adb
  - Might not want to be a device you like
- Download directly from the official market
  - android_market_api maybe
- Download from alternative market
  - Can use normal web browser
- Get it from malware repository, user group, etc

Analysis: What is an app?

- It's a zip file

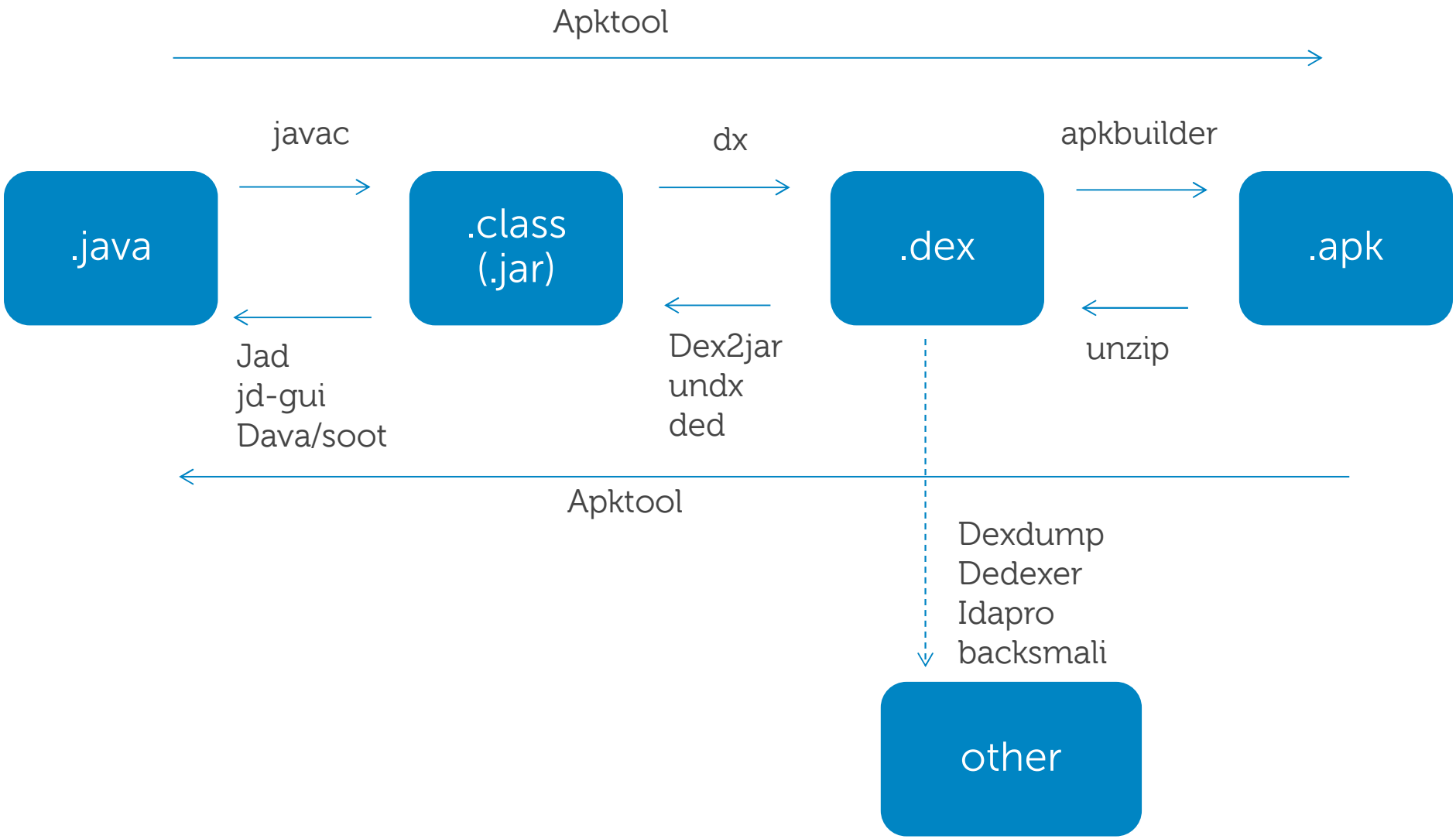
Analysis: What is an app?

- It's a zip file
- With an .apk extension (called an APK)
  - Sites may not actually deliver it with said extension
- AndroidManifest.xml
  - This is where permissions are defined
- Resources
  - images, audio, etc
- classes.dex (ALL the java classes in dex format)

Analysis: What are the tools?

- dex2jar
- ded
- Apktool
- adb
- androguard
- AXMLPrinter2
- Jad
- Jd-gui
- Dava
- soot
- backsmali
- Ida pro
- undx
- dedexer
- dexid
- droidbox

Analysis: Where to they fit?

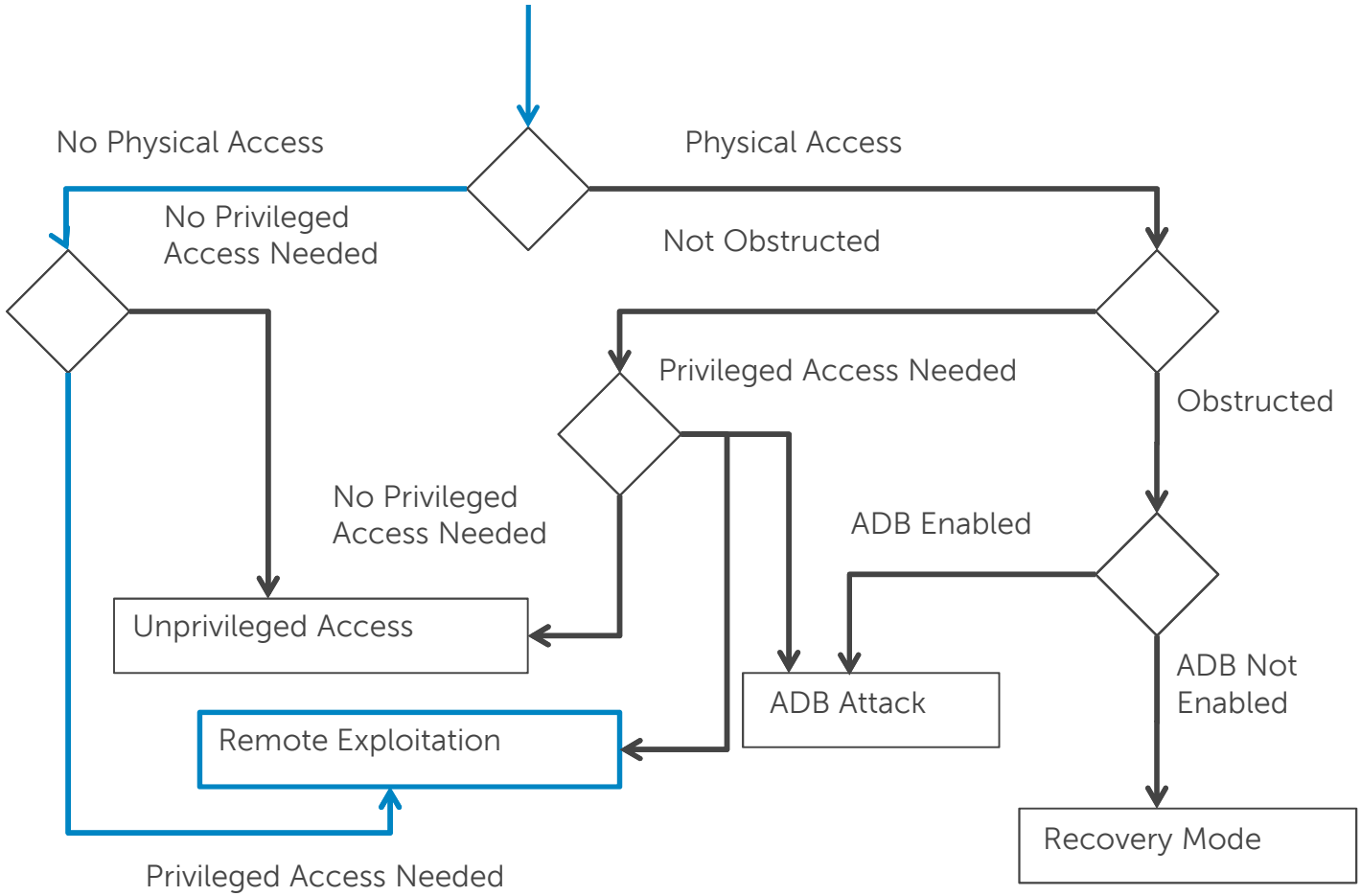


Adapted from
http://developer.android.com/guide/developing/building/index.html

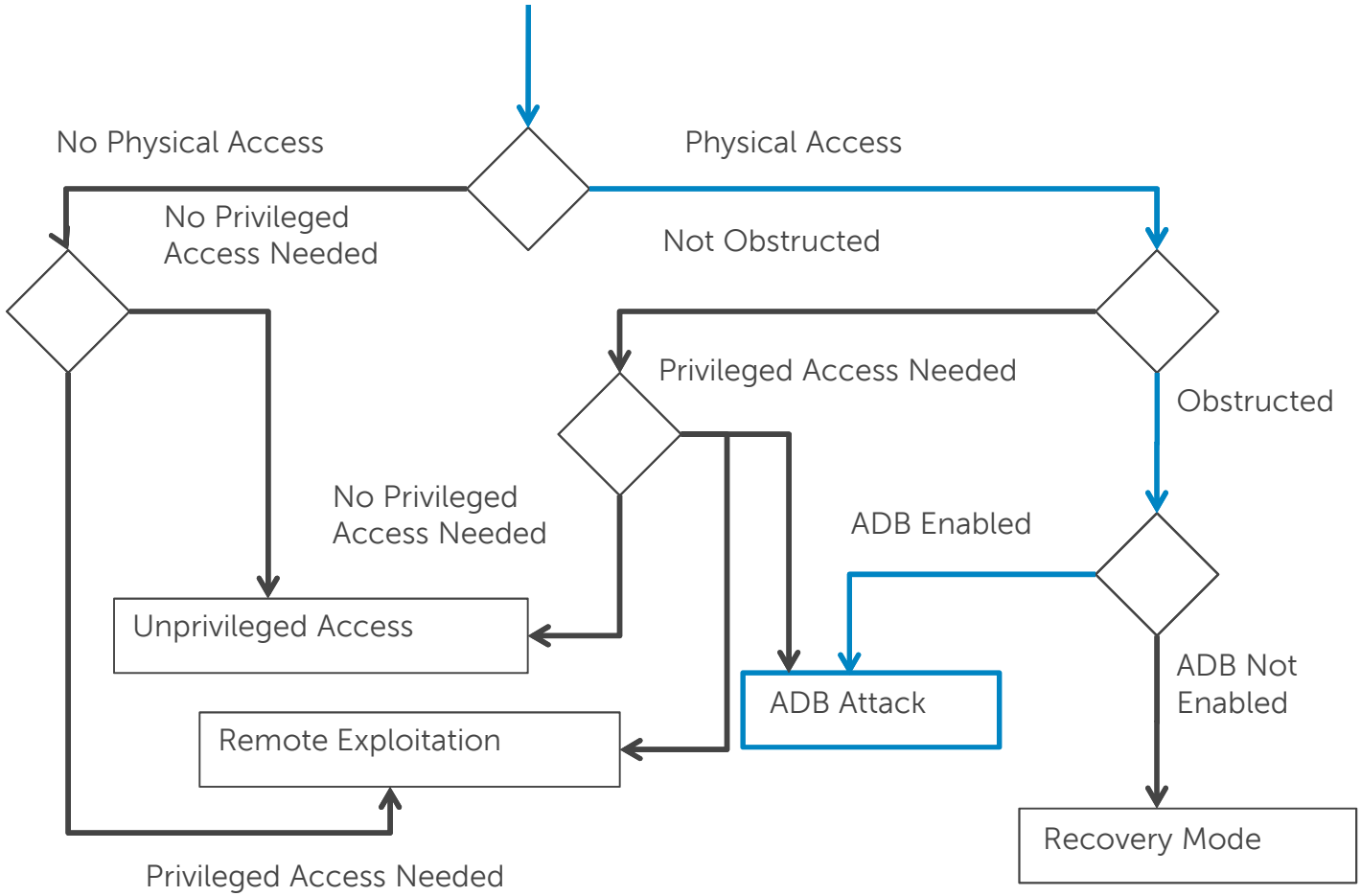
Analysis: Demos

- Sample program
- Real malware

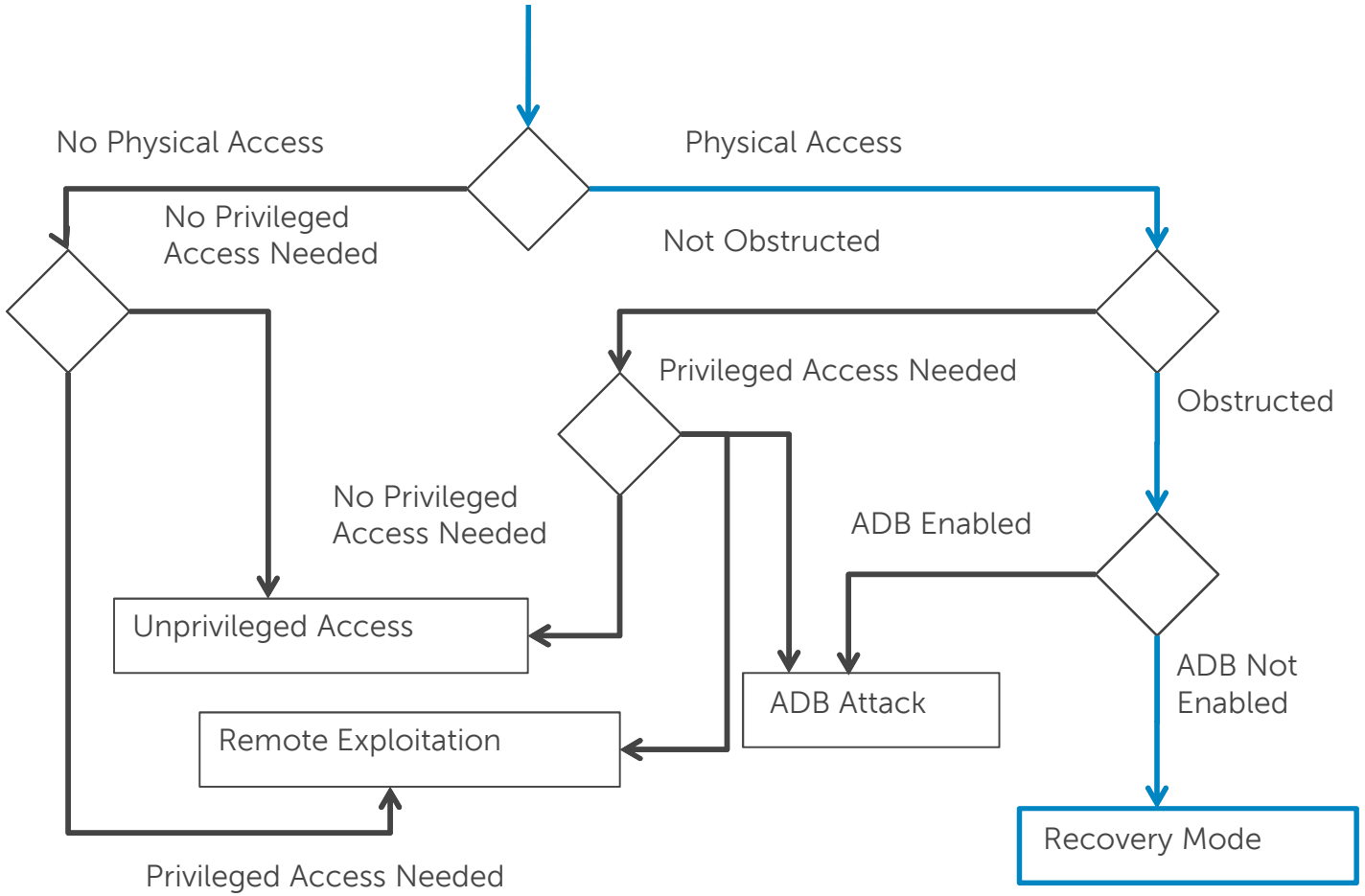
Attack Chart



Attack Chart



Attack Chart



Big Problems: network boundary

- Mobile devices as hop points
  - Such as to corp network
- Where does IDS for the phone go?

Big Problems: Who is the device admin?

Not you.

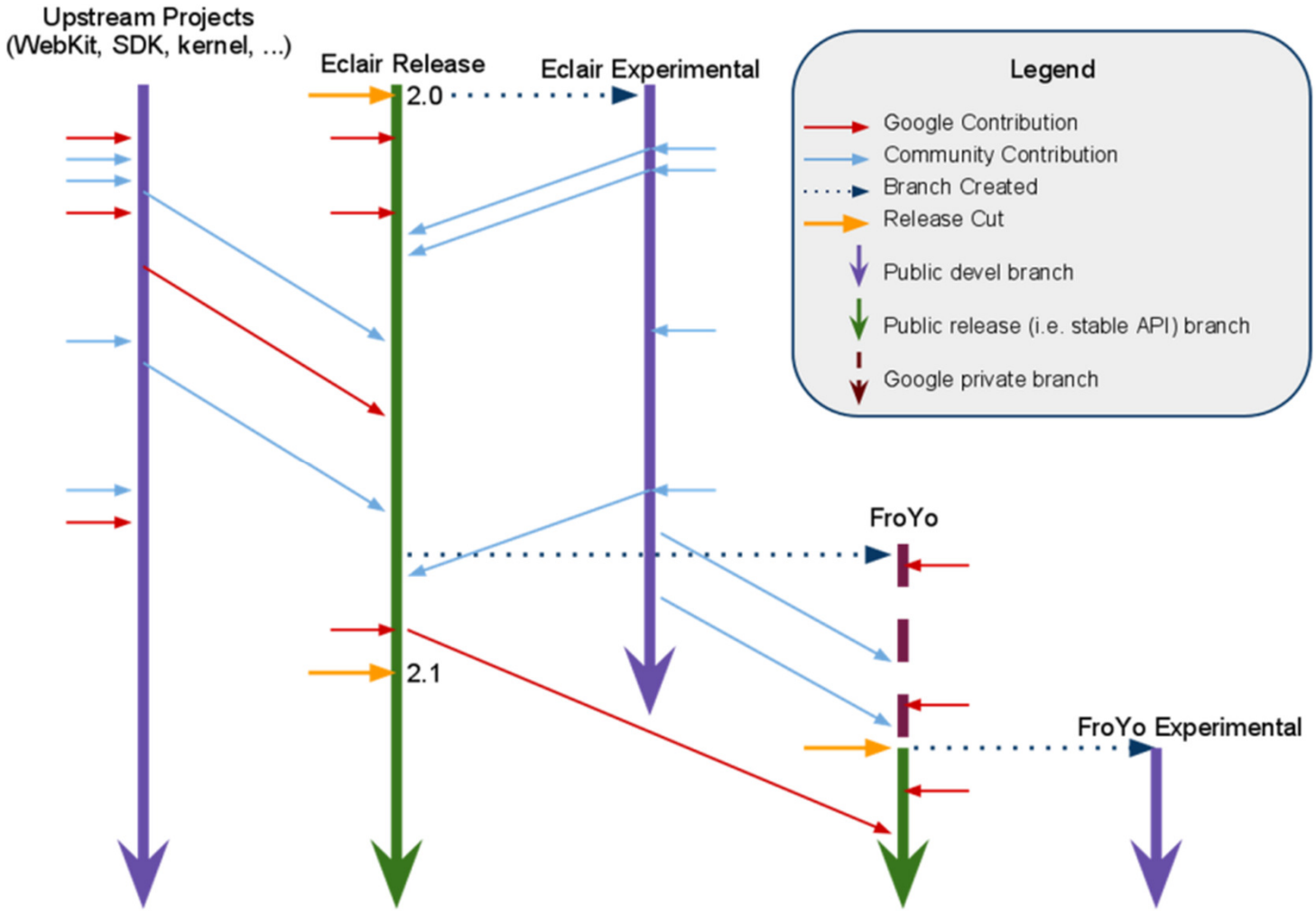
Big Problems: rooting

- Devices aren't really setup for root users
- Malware that roots for you
- Malware that targets rooted phones
  - Or custom ROMs
- Some consider rooting to undermine the security of the system
  - What little there is anyway

Big Problems: antivirus

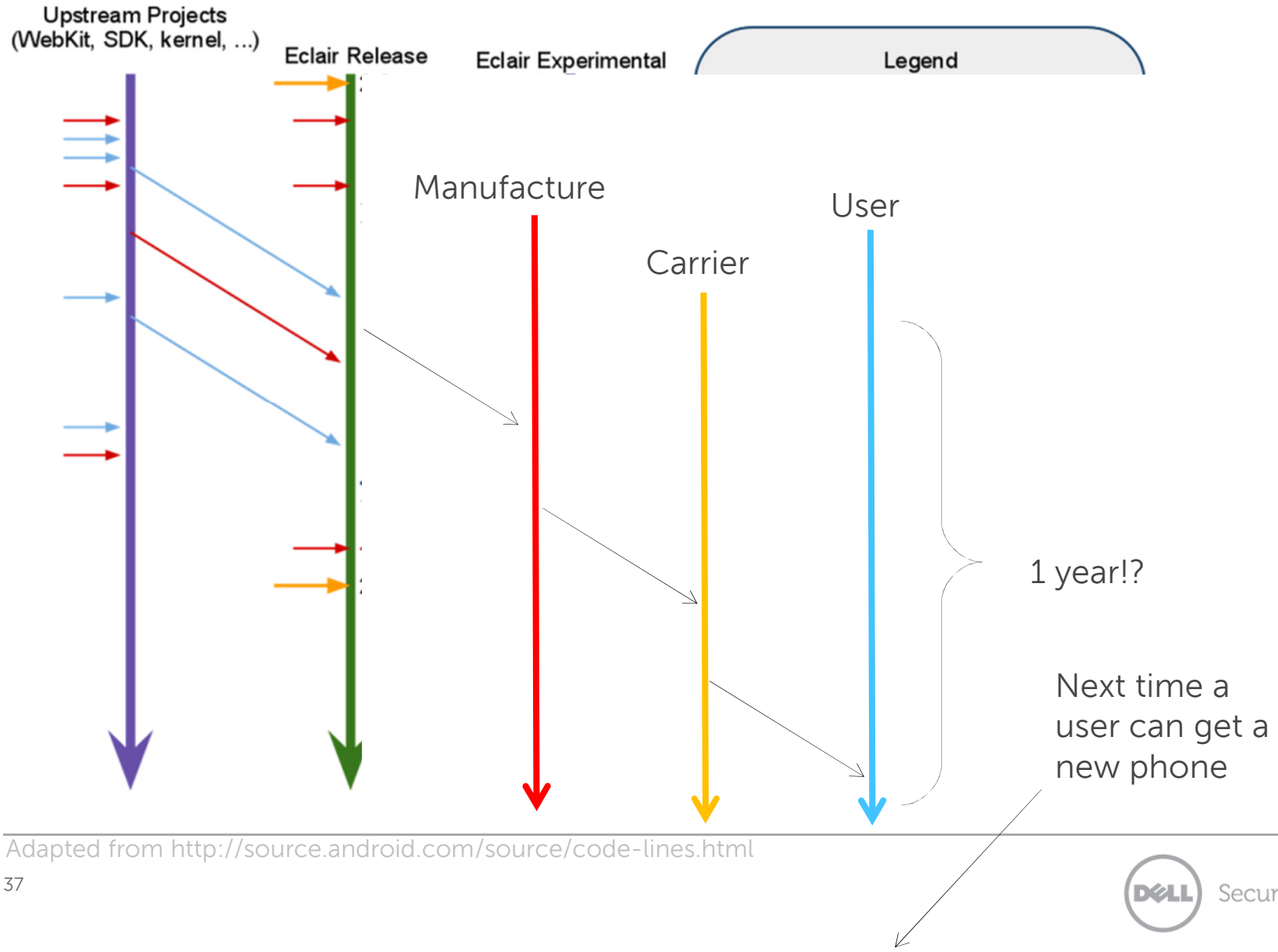
- Not easy
  - No “privileged API” available for security applications
  - Devices are often resource-constrained
  - Data plans are no longer unlimited
  - Similar arguments can be made for other security technologies

Big Problems: updates



Adapted from http://source.android.com/source/code-lines.html

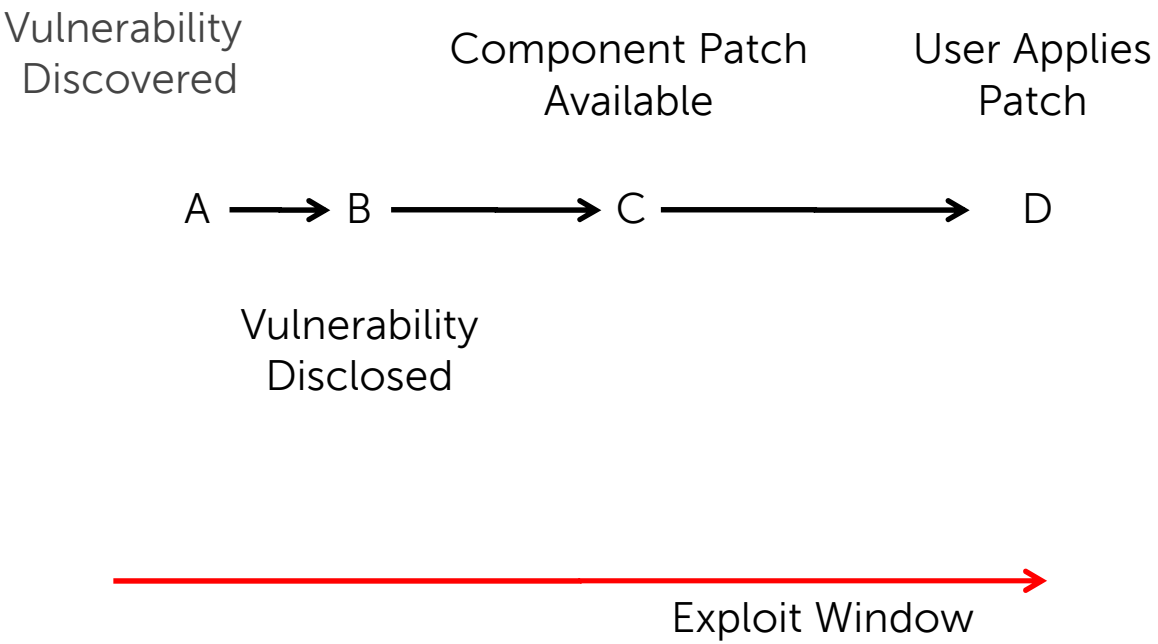
Big Problems: updates



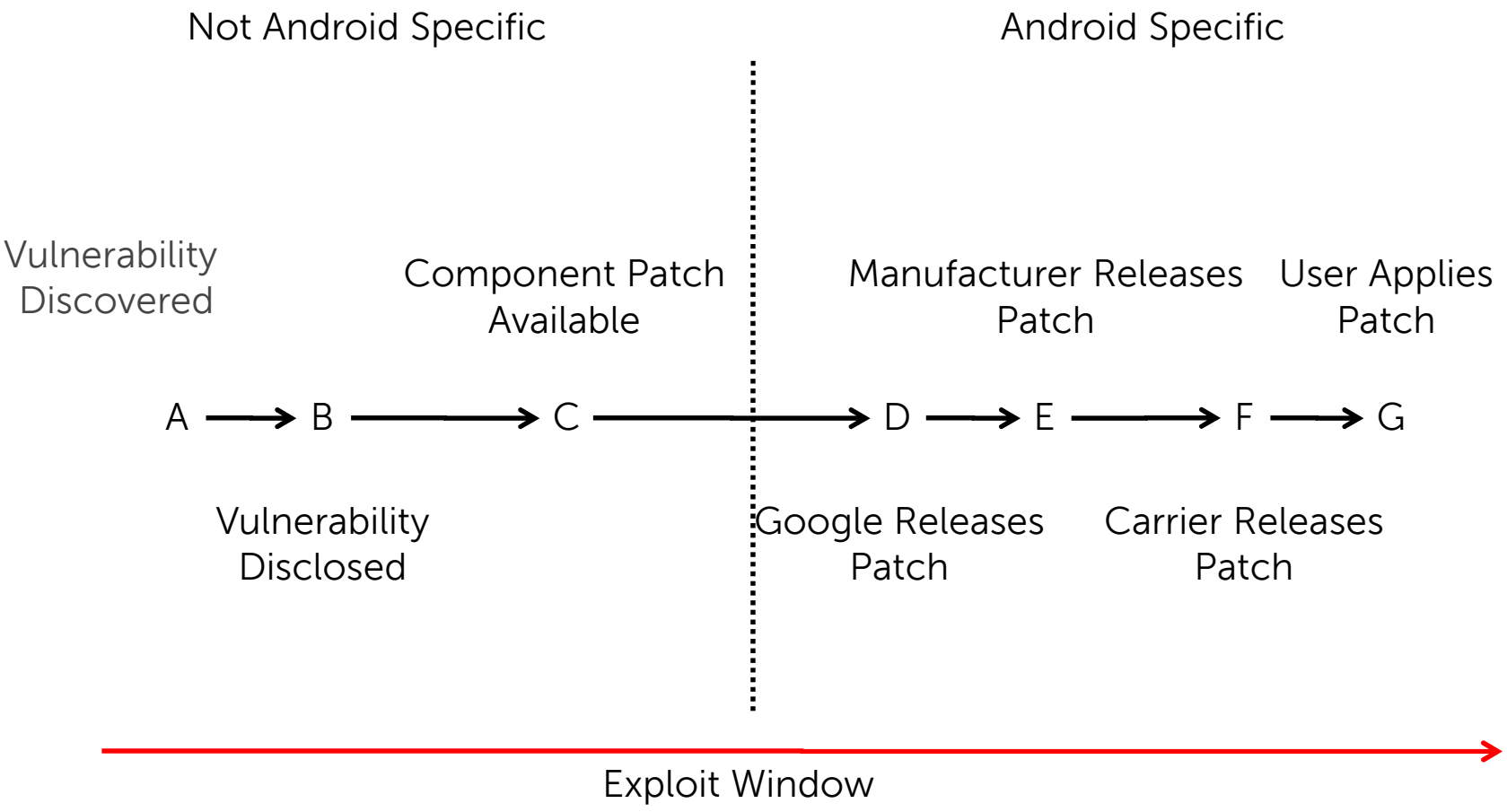
Adapted from http://source.android.com/source/code-lines.html

Big Problems: updates

Not Android Specific



Big Problems: updates



DELL SecureWorks

Big Problems: updates

- Major releases every few hundred days
- Minor every 1-2 months
- What is your phone running?

Version	Codename	Release Date	Delta (days)
1.0		9-23-2008	
1.1		2-9-2009	139
1.5	Cupcake	3-30-2009	49
1.6	Donut	9-15-2009	169
2.0	Eclair	10-26-2009	41
2.0.1		12-3-2009	38
2.1		1-12-2010	40
2.2	Froyo	5-20-2010	128
2.3	Gingerbread	12-6-2010	200
2.3.3		2-24-2011	80
2.3.4		4-28-2011	63
2.3.5		7-25-2011	88
2.3.6		9-2-2011	39

Big Problems: updates

- Major releases ev
- M
- W

hu

m

ph

Version	Codename	Release Date	Delta
2.3.6		9-2-2011	39

Nexus One denied Ice Cream Sandwich, becomes official relic of Android's yesteryears

By Joseph Volpe posted Oct 26th 2011 3:27PM

I want to play at home

- Buy a phone!
  - Or the Android SDK is easy to install and has an emulator
- Digital Forensics Research Conference challenge files:
  - http://dfrws.org/2011/challenge/index.shtml
- Honeynet “Movile Challenge”
  - http://www.honeynet.org/node/751

Thank you!

Tim Vidas

tvidas@secureworks.com